



National Information Assurance Program (NIAP) Evolution

28 September 2010

**Brian Henderson
NSA Commercial Solutions Center**

A Historical Perspective

- 1983 - 1997
 - NSA's National Computer Security Center (NCSC) used DoD TCSEC (Orange Book or DoD 5200.28-STD) criteria within the Trusted Product Evaluation Program (TPEP) (totally government funded - using government & FFRDC evaluators)
- 1997
 - NIST & NSA Implemented Trusted Technology Assessment Program (TTAP) using Orange Book and Common Criteria standards & evaluations by approved commercial labs with NSA oversight.
- 1997
 - Letter of partnership signed between NIST & NSA establishing the National Information Assurance Partnership (NIAP).

A Historical Perspective


- 1998
 - International Common Criteria Version 2.0 published
- 1999
 - CC V2.0 adopted as ISO Standard 15408
- 2000
 - NIAP/CCEVS program implemented using Common Criteria & evaluations by accredited commercial labs with government oversight/validation.
- 2007
 - NIST formally terminated the partnership. Continue to support commercial lab certification via NVLAP.
- 2009
 - New strategy announced

Common Criteria Evaluation and Validation Scheme (CCEVS)

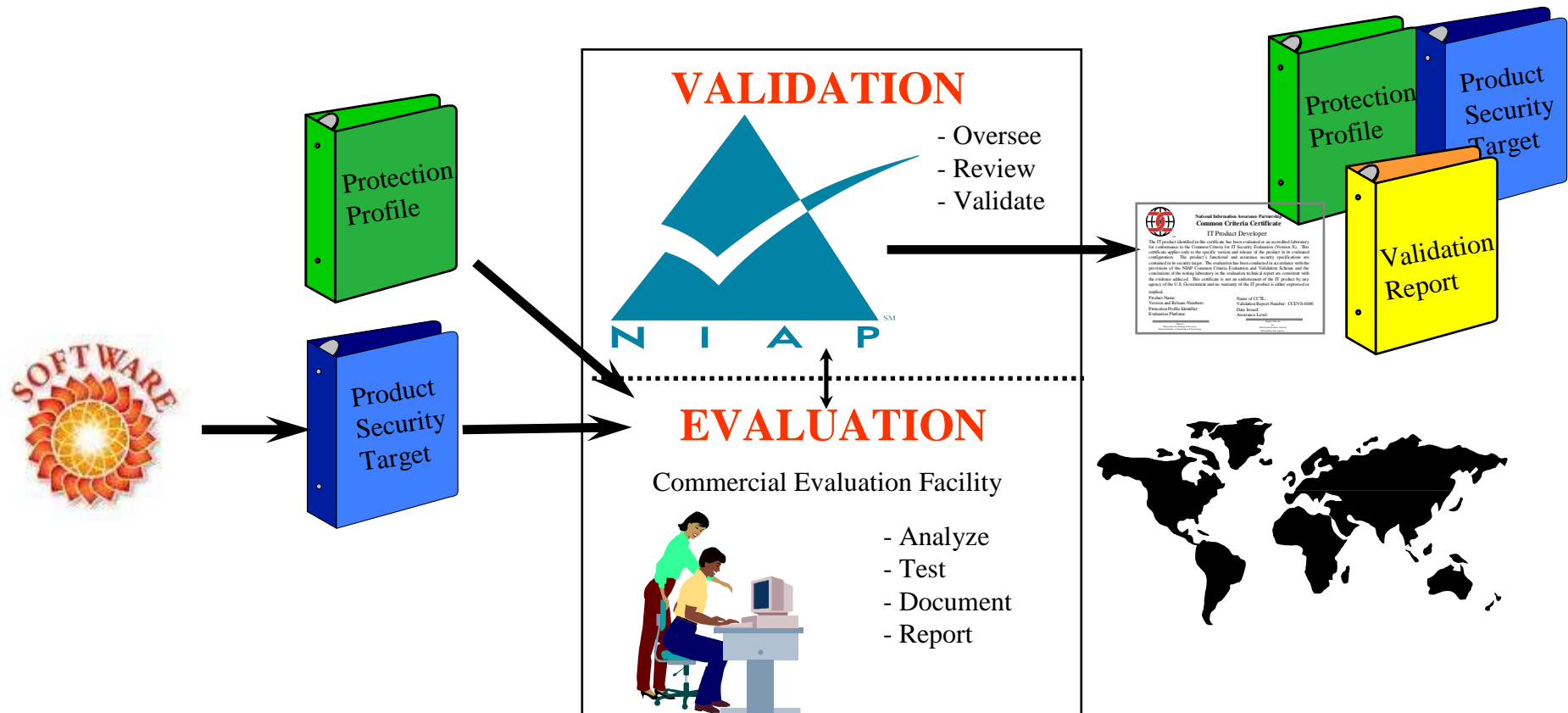
- **Objective**
 - Test Security Properties of Commercial Products
- **Approach**
 - Tests performed by Accredited Commercial Laboratories
 - Validity/Integrity of results underwritten by NIAP
 - Results posted for public access

Common Criteria Evaluation and Validation Scheme (CCEVS)

- Evaluates conformance of the security features of IT products to the *International Common Criteria (CC) for Information Technology Security Evaluation*.
- Issues Certificates to vendors for successful completion of evaluations.
 - Not an NSA or NIST endorsement
 - Not a statement about goodness of product

		National Information Assurance Partnership	
		Common Criteria Certificate	
		Vendor Name	
<p>The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version X) for conformance to the Common Criteria for IT Security Evaluation (Version X). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the product's security target. This certificate is not an endorsement of the IT product by the NSA or NIST. It is a statement of conformance to the Common Criteria.</p>			
Product Name:		Version and Release:	
Protection Profile Identifier:		Date Issued:	
Evaluation Platform:		Assurance Level:	
Director, Information Technology Laboratory National Institute of Standards and Technology		Deputy Director for Information Systems Security National Security Agency	

Evaluation Process Summary



U.S. Approved Common Criteria Testing Laboratories

- | | | |
|----|---|------------------------|
| 1. | Booz Allen Hamilton (BAH) | Linthicum, Maryland |
| 2. | Arca | Sterling, Virginia |
| 3. | Atsec | Austin, Texas |
| 4. | COACT, Inc. | Columbia, Maryland |
| 5. | Computer Sciences Corp (CSC) | Annapolis Junction, MD |
| 6. | CygnaCom Solutions, Inc. | McLean, Virginia |
| 7. | InfoGard Laboratories, Inc. | San Luis Obispo, CA |
| 8. | Science Applications Int'l Corp (SAIC) | Columbia, MD |
| 9. | DSD Information Assurance Lab (DIAL) | White Hall, WV |

CCTL Evaluation Facts

- Prices and Evaluation Time for *typical* evaluations:
 - EAL 2 (e.g. IDS, Firewall, Router, Switch)
~\$100-170K, 4-6 months
 - EAL 3 (e.g. Firewall, IDS – PP Compliant)
~\$130 -225K, 6-9 months
 - Simple EAL 4 (e.g. IDS, Firewall, Router, Switch)
~\$175K- \$300K, 7-12 months
 - Complex EAL 4 (e.g. Operating System – PP Compliant) ~300K-750K, 12-24 months
- Fixed Price Contracts generally are higher cost

Mutual Recognition Arrangement

NIAP, in conjunction with the U.S. State Dept., negotiated a Common Criteria Recognition Arrangement that:

- Provides recognition of Common Criteria certificates among 26 nations for EAL 1-4
 - Recently Estonia and Iran showing interest.
 - China and Russia attend but are not members
- Eliminates need for costly security evaluations in more than one country
- Offers excellent global market opportunities for U.S. IT industry



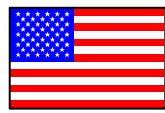
®

**Certificate
Producers**

Common Criteria Recognition Arrangement (CCRA)



Italy



US



Australia



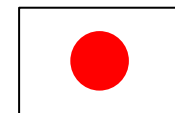
Canada



France



Germany



Japan



Netherlands



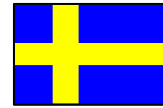
New Zealand



Norway



Spain



Sweden



South Korea



UK

**Certificate
Consumers**



Austria



**Czech
Republic**



Denmark



Finland



Greece



Hungary



Israel



India



Malaysia



Pakistan



Singapore



Turkey

Drumbeat for Change

- DSB Report; Mission Impact of Foreign Influence on DOD Software, 2007
 - Automated Vulnerability Analysis tools
 - Automated Vulnerability Reduction tools
 - Better to fix than start over
- GCN 2007
 - Focus on assessing evaluation documentation, not product security.
 - Paperwork drill, not product evaluation
 - Evaluation process opaque
 - Insufficient industry involvement
- GAO report 2006
- CSI Alliance 2004
 - Automated Testing
 - CC process assumes waterfall method, not spiral development.

FY10 NSA Information Assurance Commercial Strategy Goals

Reform National Information Assurance Partnership

- "Institute changes internally and champion changes externally that are necessary for Common Criteria (CC) to obtain valuable, consistent, and comparable results from its evaluations."
- **Why?**
 - Address long-standing criticisms
 - Improved response to client demands and technology changes.
 - Enable Commercial Solutions Partnership Program
 - Clear requirements for Acquisition Authorities



NIAP Today

- Elimination of Robustness Model
- Re-writing all current Protection Profiles
 - EAL 2
- Developing Standard Protection Profiles
- Coordinating with CCRA community
- Meeting with US Government customers
- Re-writing of NSTISSP #11

NIAP Today

– Four Priorities

- Customer Engagement
- Policy Updates
- CCv4.0
- Protection Profiles

– NIAP Metrics

- IAD Strategic Plan
- Cryptographic Interoperability Strategy Transformation (Suite B)

FY10 NSA Information Assurance Commercial Strategy Goals

Commercial Solutions Partnership Program (CSPP)

- **Develop, pilot and institute a process leading to approval of a composition of COTS products for processing classified information.**
- **Why?**
 - **GOTS products cannot compete with COTS for ease of use, rate of change, and acceptable cost for some technologies. IAD must help its customers choose and securely deploy COTS products for these technologies.**

CSPP in a Nutshell

***Solutions composed of COTS products approved
to protect classified information***

- NSA publishes CSPP “Solution Framework”
 - Unclassified, generic architecture for use cases
 - Layered, diverse products
 - At least two cryptographic layers
- “Solution Specification” and “Solution Implementation” developed by client from Solution Framework.
 - NSA Approves
- Solutions draw only from CSPP “listed” products
 - Memo of Understanding
 - Secure Sharing Suite (Suite B algorithms plus protocols, etc)
- NIAP and FIPS is “front door” for CSPP “listed” products

www.niap-ccevs.org

CCEVS Big Picture

Objectives

Validation Body

History

CC Testing Labs

Events

Announcements

CCEVS Products

Products in Evaluation

Validated Product List

Validated Protection Profiles

PP in Development

Documents and Guidance

Connection to Common Criteria Portal



QUESTIONS ?

Review of Common Criteria (CC)

Important Web Sites

CCEVS	http://www.niap-ccevs.org
NSTISSP No. 11	http://www.niap-ccevs.org/cc-scheme/faqs/
Validated Products	http://www.niap-ccevs.org/cc-scheme/vpl/
Protection Profiles	http://www.niap-ccevs.org/cc-scheme/pp/

Contact Information

Carol Houck

Director, NIAP

410-854-4458

Shaun Gilmore

Chief Validator

Michelle Brinkmeyer

Dianne Hale

Darren King

Background Info

Authorities and Policies for CSPP

- E.O. 12333, “U.S. Intelligence Activities” – Names DIRNSA as the National Manager for U.S. National Security Systems (NSS)
- NSD-42, “National Policy Security of National Security Telecommunications and Information Systems” – Establishes DIRNSA’s National Manager responsibilities including setting standards and evaluating NSS to protect them from foreign interception and exploitation.
- NSTISSP-11: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products
- CNSSP-15: National Information Assurance Policy on the use of Public Standards for the Secure Sharing of Information Among National Security Systems
 - **Establishes use of a secure sharing suite using a standard suite of security protocols and cryptographic algorithms to protect NSS information**
 - **Until 1Oct15**
 - Suite B
 - Legacy
 - NSA
 - **After 1Oct15**
 - Suite B
 - NSA
- DoDI 8523.01 Communications Security (COMSEC). Pursuant to Enclosure 2, paragraph E2.8, NSA/CSS approval of COMSEC may consist of:
 - **(2) product or system approval wherein NSA/CSS approves a set of generic solutions. In the latter case, the approved solution may consist of a combination of components. The use of this combination of components allows a user to protect information of the type specified in the NSA/CSS approval specification.”**

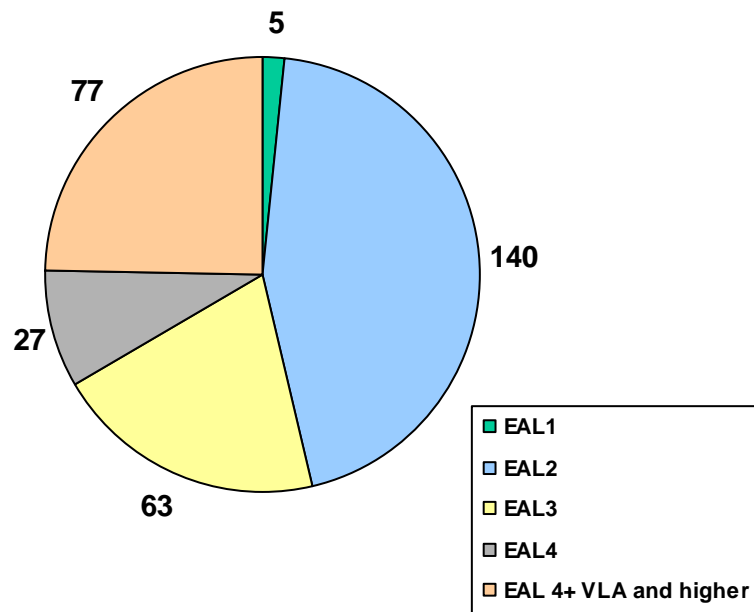
Classified or
Unclassified

New
CSPP
Approval
Process

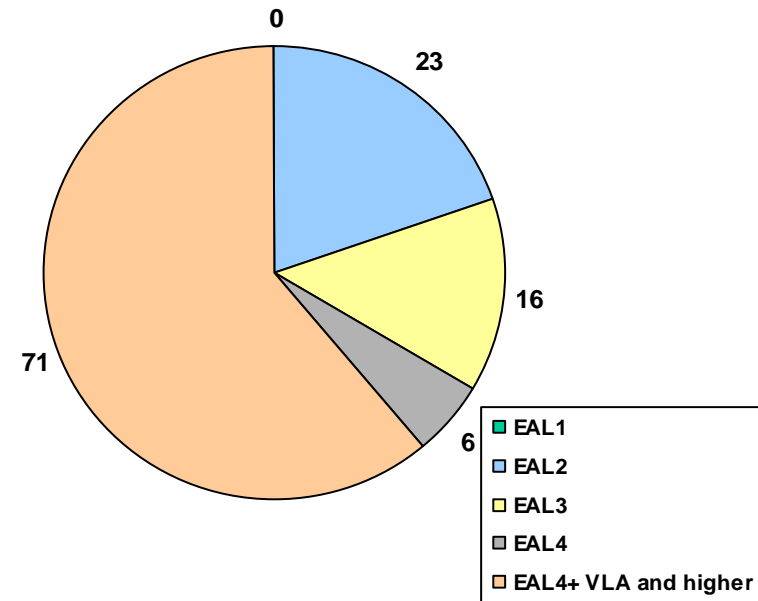
NIAP Today Evaluated Products

30 September 2009

312 Completed Product ST Evaluations



116 Product ST Evaluations in Progress



Governing Policies

- **NSTISSP 11**
 - National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products that protect national security information. Mandated purchases of these types of products be limited to those evaluated by CC, NIAP or FIPS beginning in Jul 2002
- **DoD Directive 8500.1, Oct 2002**
 - DoD policy mandating compliance with NSTISSP 11, requiring products to be evaluated or in evaluation (with successful evaluation a condition of the purchase)
- **DoD Instruction 8500.2, Feb 2003**
 - DoD policy mandating product being evaluated also conform to a Government Protection Profiles (whenever one exists)

Terminology

- Evaluation Assurance Level (EAL)
- Protection Profile (PP)
- Security Target (ST)
- Target of Evaluation (TOE)
- Evaluators
- Validators
- Evaluation Technical Report (ETR)
- Validated Products List (VPL)
- Common Criteria Testing Laboratory (CCTL)

Terminology

Evaluation Assurance Levels

- **EAL 1 – Functionally tested.** The product has been functionally tested using available off-the-shelf vendor documentation. Doesn't require vendor cooperation.
- **EAL 2 – Structurally tested.** The product has been functionally tested using available off-the-shelf vendor documentation as well as some vendor design documentation to support more complete functional testing. Requires vendor co-operation with delivery of design information.
- **EAL 3 – Methodically tested and checked.** The product has been functionally tested with more insight into the design and more test coverage. Developer must provide evidence of a search for obvious flaws.
- **EAL 4 – Methodically designed, tested and reviewed.** The product has been functionally tested with even more insight into the design and more comprehensive test coverage. Testing supported by independent search for obvious vulnerabilities (accomplished by NIAP lab and vendor)

(NOTE: EAL 4 is the highest level that is mutually recognized by the Common Criteria Recognition Arrangement (CCRA).)

Terminology

Evaluation Assurance Levels

- **EAL 5 – Semi-formally designed and tested.** In addition to more evidence provided by the vendor, the product must also have been developed with a rigorous development approach. Beginnings of use of formal methods and covert channel analysis and modular design. **Independent search for vulnerabilities** by attacker with moderate attack potential is **accomplished by NSA, I7.**
- **EAL 6 – Semi-formally verified design and tested.** Formal methods and systematic covert channel analysis required. Product must be modular and layered in design. Independent search for vulnerabilities by attacker with high attack potential is accomplished by NSA.
- **EAL 7 – Formally verified design and tested.** More formal methods and systematic covert channel analysis required. Product must be modular and layered in design. Independent search for vulnerabilities by attacker with high attack potential is accomplished by NSA. The complexity of the products design must be minimized. Complete independent confirmation of developer test results.

Is NIAP Improving Security?

YES!

- Product Evaluations resulting in Improved Product Security
 - ~ 35-40% of products evaluated resulted in new release or patch to fix flaw
 - Number and severity of flaws mirror Evaluation Assurance Level
 - Conformance to U.S. Government Protection Profiles drove ~90% of security additions and enhancements
- Resultant product used across Government and Commercial communities

NIAP Reform

- **U.S. Government Standard Protection Profile**
 - Necessary set of security capabilities for given technology.
 - Focus on measurable, repeatable results.
 - Less emphasis on documentation, more on tool output
 - Eliminate “robustness”
 - EAL1 – 2
 - Clearer expression of technical requirements
 - Closer partnership with Industry on PP development
 - Interim PPs the first step...Sixteen Interim Protection Profiles in review or in coordination.

Disk Encryptor (Data at Rest)

Wireless LAN

Wireless Client

VPN Gateway and Client

Firewall

OS

IDS

Database

Enterprise Security M_c

USB Encryption

